LIE METHODS IN GROWTH OF GROUPS AND GROUPS OF FINITE WIDTH

LAURENT BARTHOLDI AND ROSTISLAV I. GRIGORCHUK

Abstract. In the first, mostly expository, part of this paper, a graded Lie algebra is associated to every group G given with an N-series of subgroups. The asymptotics of the Poincaré series of this algebra give estimates on the growth of the group G. This establishes the existence of a gap between polynomial growth and growth of type $e^{\sqrt{n}}$ in the class of residually–p groups, and gives examples of finitely generated p–groups of uniformly exponential growth.

In the second part, we produce two examples of groups of finite width and describe their Lie algebras, introducing a notion of *Cayley graph* for graded Lie algebras. We compute explicitly their lower central and dimensional series, and outline a general method applicable to some other groups from the class of branch groups.

These examples produce counterexamples to a conjecture on the structure of just-infinite groups of finite width.

1. Introduction

The main goal of this paper is to present new examples of groups of finite width and to give a method of proving that some groups from the class of branch groups have finite width. This provides examples of groups of finite width with a completely new origin and answers a question asked by several mathematicians. We also give new examples of Lie algebras of finite width associated to the groups mentioned above.

The first group we study, $\mathfrak{G}$, was constructed in [Gri80] where it was shown to be an infinite torsion group; later in [Gri84] it was shown to be of intermediate growth. The second group, $\widetilde{\mathfrak{G}}$, was already considered by the second author in 1979, but was rejected at that time for not being periodic. We now know that it also has intermediate growth [BG99] and finite width.

Our interest in the finite width property comes from the theory of growth of groups. Another important area connected to this property is the theory of finite p-groups and the theory of pro-p-groups; see [Sha95b], [Sha95a, §8]

1991 *Mathematics Subject Classification.* 20F50,20F14,17B50,16P90.

The authors express their thanks to the Swiss National Science Foundation; the second author thanks the Russian Fund for Fundamental Research, research grant 01-00974 for its support.

and [KLP97] with its bibliography. More precisely, the following was discussed by many mathematicians and stated by Zel'manov in Castelvecchio in 1996 [Zel96]:

Conjecture 1.1. *Let G be a just-infinite pro-p-group of finite width. Then G is either solvable, p-adic analytic, or commensurable to a positive part of a loop group or to the Nottingham group.*

Our computations disprove this conjecture by providing a counter-example, the profinite completion of $\mathfrak{G}$ (it is a pro-p-group with $p = 2$). Note that it exhibits a behaviour specific to positive characteristic: indeed it was proved by Martinez and Zel'manov in [MZ99] that unipotence and finite width imply local nilpotence.

Before we give the definition of a group of finite width, let us recall a classical construction of Magnus [Mag40], described for instance in [HB82, Chapter VIII]. Given a group G and $\{G_n\}_{n=1}^{\infty}$ an N-series (i.e. a series of normal subgroups with $G_1 = G$, $G_{n+1} \leq G_n$ and $[G_m, G_n] \leq G_{m+n}$ for all $m, n \geq 1$), there is a canonical way of associating to G a graded Lie ring

$$\mathcal{L}(G) = \bigoplus_{n=1}^{\infty} L_n, \tag{1}$$

where $L_n = G_n/G_{n+1}$ and the bracket operation is induced by commutation in G. Possible examples of N-series are the lower central series $\{\gamma_n(G)\}_{n=1}^{\infty}$; for an integer p, the *lower p-central series* given by $P_1(G) = G$ and $P_{n+1}(G) = P_n(G)^p[P_n(G), G]$; and, for a field $\Bbbk$, the series of $\Bbbk$-*dimension subgroups* $\{G_n\}_{n=1}^{\infty}$ defined by

$$G_n = \{g \in G |\, g - 1 \in \Delta^n\}, \qquad n = 1, 2, \dots$$

where Δ is the augmentation (or fundamental) ideal of the group algebra $\Bbbk[G]$.

Tensoring the $\mathbb{Z}$-modules L_n with a suitable field $\Bbbk$, we obtain in (1) a graded Lie algebra $\mathcal{L}_{\Bbbk}(G)$. In case the N-series chosen satisfies the additional condition $G_n^p \leq G_{pn}$, and $\Bbbk$ is a field of characteristic p, the algebra $\mathcal{L}_{\Bbbk}(G)$ will then be a p-algebra or *restricted algebra*; see [Jac41] or [Jac62, Chapter V], the Frobenius operation on $\mathcal{L}_{\Bbbk}(G)$ being induced by raising to the power p in G. In this case the quotients G_n/G_{n+1} are elementary p-groups.

Many properties of a group are reflected in properties of its corresponding Lie algebra. For instance, one of the most important results obtained using the Lie method is the theorem of Zel'manov [Zel95a] asserting that if the Lie algebra $\mathcal{L}_{\mathbb{F}_p}(G)$ associated to the dimension subgroups of a finitely generated periodic residually-p group G satisfies a polynomial identity then the group G is finite ($\mathbb{F}_p$ is the prime field of characteristic p). This result gives in fact a positive solution to the Restricted Burnside Problem [VZ93, Zel95b, VZ96, Zel97]. Another example is the criterion of analyticity of pro-p-groups discovered by Lazard [Laz65].

The Lie method also applies to the theory of growth of groups, as was first observed in [Gri89]. There the second author proved that in the class of residually-p groups there is a gap between polynomial growth and growth of type $e^{\sqrt{n}}$. This result was then generalized in [LM91, Theorem D] to the class of residually-nilpotent groups, and in [CG97] the Lie method was also used to prove that certain one-relator groups with exponential-growth Lie algebra $\mathcal{L}_{\Bbbk}(G)$ have uniformly exponential growth. If a group G is finitely generated, then its Lie algebra $\mathcal{L}_{\Bbbk}(G) = \bigoplus L_n \otimes \Bbbk$ is also finitely generated, and the growth of $\mathcal{L}_{\Bbbk}(G)$ is by definition the growth of the sequence $\{b_n = \dim(L_n \otimes \Bbbk)\}_{n=1}^{\infty}$.

The investigation of the growth of graded algebras related to groups has its own interest and is related to other topics. One of the first results in this direction is the Golod-Shafarevich inequality [GS64] which plays an important role in group, number and field theories. The idea of Golod and Shafarevich was used by Lazard in the proof of the aforementioned criterion of analyticity (he even used the notation 'gosha' for the growth of the algebras). Vershik and Kaimanovich observed the relation between the growth of gosha, amenability, and asymptotic behaviour of random walks (see Section 4 below).

For our purposes it will be sufficient to consider only the fields $\mathbb{Q}$ and $\mathbb{F}_p$. Let G_n be the corresponding series of dimension subgroups, which is also an N-series, and let $\mathcal{L}_{\Bbbk}(G)$ be the associated Lie algebra. If $\mathcal{L}_{\Bbbk}(G)$ is of polynomial growth of degree $d \geq 0$, then the growth of G is at least $e^{n^{1-1/(d+2)}}$, and if $\mathcal{L}_{\Bbbk}(G)$ is of exponential growth, then G is of uniformly exponential growth.

If $\Bbbk = \mathbb{Q}$ and G is residually-nilpotent and $b_n = 0$ for some n, then G is nilpotent; indeed G_n must be finite for that n, whence $\gamma_n(G)$ is finite too, and since $\bigcap_{k\geq 1} \gamma_k(G) = 1$ this implies that $\gamma_N(G) = 1$ for some N. It follows that G has polynomial growth [Mil68]. In fact polynomial growth is equivalent to virtual nilpotence [Gro81a].

If $\Bbbk = \mathbb{F}_p$ and G is a residually-p group and $b_n = 0$ for some n, then G is a linear group over a field, by Lazard's theorem [Laz65] and therefore has either polynomial or exponential growth, by the Tits alternative [Tit72].

Finally, if $b_n \geq 1$ for all n then, independent of $\Bbbk$, the growth of G is at least $e^{\sqrt{n}}$. Keeping in mind that polynomial growth $b_n \sim n^d$ of $\mathcal{L}_{\Bbbk}(G)$ implies a lower bound $e^{n^{1-1/(d+2)}}$ for the growth of G, we conclude that examples of groups with growth exactly $e^{\sqrt{n}}$ are to be found amongst the class of groups for which the sequence $\{b_n\}_{n=1}^{\infty}$ is uniformly bounded, or at least bounded in average. This key observation leads to the notion of *groups of finite width.* We present two versions of the definition:

Definition 1.2. Let G be a group and $\Bbbk \in \{\mathbb{Q}, \mathbb{F}_p\}$ a field. If $\Bbbk = \mathbb{Q}$, assume G is residually-nilpotent; if $\Bbbk = \mathbb{F}_p$, assume G is residually-p.

1. G has *finite C-width* if there is a constant K with $[\gamma_n(G) : \gamma_{n+1}(G)] \leq K$ for all n.

2. G has *finite D-width with respect to* $\Bbbk$ if there is a constant K with $b_n \leq K$ for all n, where $\{b_n\}_{n=1}^\infty$ is the growth of $\mathcal{L}_\Bbbk(G)$ constructed from the dimension subgroups.

A third notion can be defined, that of *finite averaged width*; see [Gri89] or [KLP97, Definition I.1.ii]. From our point of view D-width is more natural; but the first notion is more commonly used in the theory of finite p-groups and pro-p-groups, see for instance [KLP97, Definition I.1.i]. The examples we will produce are of finite width according to both definitions. That one of our groups has finite width was conjectured in [Gri89]; it was proven that the numbers b_n are bounded in average. Rozhkov then confirmed this conjecture in [Roz96a] by computing explicitly the b_n; but the proof had gaps, one of which was filled in [Roz96b]. We fix another gap in the "Technical Lemma 4.3.2" of [Roz96b] while simplifying and clarifying Rozhkov's proof, and also outline a general method, connected to ideas of Kaloujnine [Kal46].

We recall in the next section known notions on algebras associated to groups, and construct in Section 3 a torsion group of uniformly exponential growth. Section 5 describes a class of groups acting on rooted trees, and the next two sections detail for two specific examples the indices of the lower central and dimensional series. More specifically, we compute in Theorem 6.6 and 7.6 the indices of these series for the group $\mathfrak{G}$ and an overgroup $\widetilde{\mathfrak{G}}$. We also obtain in the process the structure of the Lie algebras $L(\mathfrak{G})$ (associated to the lower central series) and $\mathcal{L}_{\mathbb{F}_2}(\mathfrak{G})$ (associated to the dimension series) in Theorem 6.7, and that of $L(\widetilde{\mathfrak{G}})$ and $\mathcal{L}_{\mathbb{F}_2}(\widetilde{\mathfrak{G}})$ in Theorem 7.7. They are described using Cayley graphs of Lie algebras, see Subsection 6.1.

Throughout this paper groups shall act on the left. We use the notational conventions $[x,y] = xyx^{-1}y^{-1}$ and $x^y = yxy^{-1}$.

Both authors wish to thank Aner Shalev and Efim Zelmanov for their interest and generous contribution through discussions.

2. Growth of Groups and Associated Graded Algebras

Let G be a group, $\{\gamma_n(G)\}_{n=1}^\infty$ the lower central series of G, $\Bbbk \in \{\mathbb{Q}, \mathbb{F}_p\}$ a prime field, $\Delta = \ker(\varepsilon) < \Bbbk[G]$ the augmentation ideal, where $\varepsilon(\sum k_i g_i) = \sum k_i$ is the augmentation map $\Bbbk[G] \to \Bbbk$, and $\{G_n\}_{n=1}^\infty$ the series of dimension subgroups of G [Zas40, Jen41]. Recall that

$$G_n = \{g \in G |\, g - 1 \in \Delta^n\}.$$

The restrictions we impose on $\Bbbk$ are not important, as G_n depends only on the characteristic of $\Bbbk$. We suppose throughout that G is residually-nilpotent if $\Bbbk = \mathbb{Q}$ and is residually-p if $\Bbbk = \mathbb{F}_p$.

If $\Bbbk = \mathbb{Q}$, then G_n is the isolator of $\gamma_n(G)$, as was proved in [Jen55] (see also [Pas77, Theorem 11.1.10] or [Pas79, Theorem IV.1.5]); i.e.

$$G_n = \sqrt{\gamma_n(G)} = \{g \in G |\, g^\ell \in \gamma_n(G) \text{ for an } \ell \in \mathbb{N}\}.$$

Note that in [Pas77] these results are stated for finite p-groups. They nevertheless hold in the more general setting of residually-nilpotent or residually-p groups.

If $\Bbbk = \mathbb{F}_p$, then $\gamma_n(G) \leq G_n \leq \sqrt{\gamma_n(G)}$, and the G_n can be defined in several different ways, for instance by the relation

$$G_n = \prod_{i \cdot p^j \geq n} \gamma_i^{p^j}(G)$$

due to Lazard [Laz53], or recursively as

$$G_n = [G, G_{n-1}] G^p_{\lceil n/p \rceil}, \tag{2}$$

where $\lceil n/p \rceil$ is the least integer greater than or equal to n/p. In characteristic p, the series $\{G_n\}_{n=1}^{\infty}$ is called the lower p-central, Brauer, Jennings, Lazard or Zassenhaus series of G. The quotients G_n/G_{n+1} are elementary abelian p-groups and define the fastest-decreasing central series with the property $G_n^p \leq G_{np}$ [Jen55].

Let

$$\mathcal{A}(G) = \mathcal{A}_{\Bbbk}(G) = \bigoplus_{n=0}^{\infty} \Delta^n / \Delta^{n+1}$$

be the associative graded algebra with product induced linearly from the group product (see [Pas77, Pas79] for more details).

If $\Bbbk = \mathbb{Q}$, consider the following graded Lie algebras over $\Bbbk$:

$$\mathcal{L}(G) = \bigoplus_{n=1}^{\infty} \big(G_n/G_{n+1} \otimes_{\mathbb{Z}} \mathbb{Q} \big), \qquad L(G) = \bigoplus_{n=1}^{\infty} \big(\gamma_n(G)/\gamma_{n+1}(G) \otimes_{\mathbb{Z}} \mathbb{Q} \big).$$

If $\Bbbk = \mathbb{F}_p$, consider the restricted Lie $\mathbb{F}_p$-algebra

$$\mathcal{L}_p(G) = \bigoplus_{n=1}^{\infty} \big(G_n/G_{n+1} \big).$$

Then Quillen's Theorem [Qui68] asserts that $\mathcal{A}(G)$ is the universal enveloping algebra of $\mathcal{L}(G)$ in characteristic 0 and is the universal p-enveloping algebra of $\mathcal{L}_p(G)$ in positive characteristic.

Let us introduce the following numbers:

$$a_n(G) = \dim_{\Bbbk}(\Delta^n / \Delta^{n+1}), \qquad b_n(G) = \operatorname{rank}(G_n/G_{n+1}).$$

Here by the rank of the G-module M we mean the torsion-free rank $\dim_{\mathbb{Q}}(M \otimes \mathbb{Q})$ in characteristic 0 and the p-group rank $\dim_{\mathbb{F}_p}(M \otimes \mathbb{F}_p)$, equal to the minimal number of generators, in positive characteristic. Note that in zero-characteristic $b_n = \operatorname{rank}(\gamma_n(G)/\gamma_{n+1}(G))$, because the natural map

$$\gamma_n(G)/\gamma_{n+1}(G) \to G_n/G_{n+1}$$

has finite kernel and cokernel.

The following result is due to Jennings. The case $\Bbbk = \mathbb{F}_p$ appears in [Jen41] and the case $\Bbbk = \mathbb{Q}$ appears in [Jen55]; but see also [Pas77, Theorem 3.3.6 and 3.4.10].

$$\sum_{n=0}^{\infty} a_n(G)t^n = \begin{cases} \prod_{n=1}^{\infty}\left(\frac{1-t^{pn}}{1-t^n}\right)^{b_n(G)} & \text{if } \Bbbk = \mathbb{F}_p, \\ \prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{b_n(G)} & \text{if } \Bbbk = \mathbb{Q}. \end{cases} \tag{3}$$

The series $\sum_{n=0}^{\infty} a_n(G)t^n$ is the Hilbert-Poincaré series of the graded algebra $\mathcal{A}(G)$. The equation (3) expresses this series in terms of the numbers $b_n(G)$; the relation between the sequences $\{a_n(G)\}_{n=0}^{\infty}$ and $\{b_n(G)\}_{n=1}^{\infty}$ is quite complicated. We shall be interested in asymptotic growth of series, in the following sense:

Definition 2.1. Let f and g be two functions $\mathbb{R}_+ \to \mathbb{R}_+$. We write $f \precsim g$ if there is a constant $C > 0$ such that $f(x) \le C + Cg(Cx + C)$ for all $x \in \mathbb{R}_+$, and write $f \sim g$ if $f \precsim g$ and $g \precsim f$.

A series $\{a_n\}_{n=0}^{\infty}$ defines a function $f : \mathbb{R}_+ \to \mathbb{R}_+$ by $f(x) = a_{\lfloor x \rfloor}$, and for two series $a = \{a_n\}$ and $b = \{b_n\}$ we write $a \precsim b$ and $a \sim b$ when the same relations hold for their associated functions.

The main facts are presented in the following statement:

Proposition 2.2. *Let $\{a_n\}$ and $\{b_n\}$ be connected by the one of the relations (3). Then*

1. *$\{b_n\}$ grows exponentially if and only if $\{a_n\}$ does, and we have*
$$\limsup_{n\to\infty} \frac{\ln a_n}{n} = \limsup_{n\to\infty} \frac{\ln b_n}{n}.$$
2. *If $b_n \sim n^d$ then $a_n \sim e^{n^{(d+1)/(d+2)}}$.*

Proof. We first suppose $\Bbbk = \mathbb{Q}$, and prove Part 1 following [Ber83]. Let $A = \limsup(\ln a_n)/n$ and $B = \limsup(\ln b_n)/n$. Clearly $A \ge B$ as $a_n \ge b_n$ for all n; we now prove that $A \le B$. Define

$$f(z) = \prod_{n=1}^{\infty}(1 - e^{-nz})^{-b_n},$$

viewed as a complex analytic function in the half-plane $\Re(z) > B$. We have $|1 - e^{-nz}|^{-1} \le (1 - e^{-n\Re z})^{-1}$, from which $|f(z)| \le f(\Re z)$. Now applying the Cauchy residue formula,

$$a_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(u+iv)e^{n(u+iv)}dv \le \frac{1}{2\pi}\int_{-\pi}^{\pi} |f(u+iv)|e^{nu}dv \le e^{nu}f(u)$$

for all $u > B$, so

$$A = \limsup_{n\to\infty} \frac{\ln a_n}{n} \le \limsup_{u>B,n\to\infty}\left(u + \frac{\ln f(u)}{n}\right) = B.$$

For $\Bbbk = \mathbb{F}_p$, Part 1 holds *a fortiori.*

Part 2 for $\Bbbk = \mathbb{Q}$ is a consequence of a result by Meinardus ([Mei54]; see also [And76, Theorem 6.2]). More precisely, when $b_n = n^d$, his result implies that

$$a_n \approx \frac{e^{\zeta'(-d)}}{\sqrt{2\pi(d+2)n}} \left(\frac{(d+1)!\zeta(d+2)}{n}\right)^{\frac{1-2\zeta(-d)}{2+4d}} e^{n\frac{d+2}{d+1}\left(\frac{(d+1)!\zeta(d+2)}{n}\right)^{\frac{1}{1+2d}}},$$

where '$\approx$' means that the quotient tends to 1 as $n \to \infty$, and ζ is the Riemann zeta function.

We sketch the proof for $\Bbbk = \mathbb{Q}$ below: we suppose that $b_n \sim n^d$, so $A = B = 0$ by Part 1, and compute

$$\begin{aligned} \frac{d}{du} \ln f(u) = \sum_{n=1}^{\infty} -b_n \frac{-ne^{-nu}}{1 - e^{-nu}} \quad &\sim \quad \frac{1}{u^{d+2}} \sum_{n=1}^{\infty} \frac{(nu)^{d+1}}{e^{nu} - 1} u \\ &\sim \quad \frac{1}{u^{d+2}} \int_0^{\infty} \frac{w^{d+1}}{e^w - 1} dw = \frac{C}{u^{d+2}}. \end{aligned}$$

Thus $\ln f(u) \sim C/u^{d+1}$, and the inequality

$$\log a_n \leq nu + \log f(u) \sim nu + C/u^{d+1}$$

is tight by the saddle-point principle when the right-hand side is minimized. This is done by choosing $u = n^{-1/(d+2)}$, whence as claimed $\log a_n \sim n^{1-1/(d+2)}$.

Finally, we show that (3) yields the same asymptotics when $\Bbbk = \mathbb{F}_p$ as when $\Bbbk = \mathbb{Q}$. Clearly

$$\prod_{n=1}^{\infty} (1 + t^n)^{b_n} \leq \prod_{n=1}^{\infty} (1 + t^n + \cdots + t^{(p-1)n})^{b_n} \leq \prod_{n=1}^{\infty} (1 + t^n + \dots)^{b_n}$$

for all $p \geq 2$, where for two power series $\sum e_t^n$ and $\sum f_n t^n$ the inequality $\sum e_t^n \leq \sum f_n t^n$ means that $e_n \leq f_n$ for all n. It thus suffices to consider the case $p = 2$. For this purpose define

$$g(z) = \prod_{n=1}^{\infty} (1 + e^{-nz})^{b_n},$$

and compare the series developments of $\log(f)$ and $\log(g)$ in e^{-z}. From $-\log(1 - z) = \sum_{n \geq 1} \frac{z^n}{n}$ it follows that

$$\begin{aligned} \log f(z) &= \sum_{n \geq 1} f_n e^{-nz}, \quad f_n = \sum_{d|n} \frac{1}{d}, \\ \log g(z) &= \sum_{n \geq 1} g_n e^{-nz}, \quad g_n = \sum_{d|n} \frac{(-1)^{d+1}}{d}, \end{aligned}$$

so both series have the same odd-degree coefficients, and thus $\log f \sim \log g$. Their exponentials then have the same asymptotics; more precisely, $f_n \leq g_{2n-1}$ for all n, so $e^z \log f(2z) \leq \log g(z)$ termwise, and $f(2z) \leq g(z)$. $\square$

2.1. **Growth of Groups.** Let G be a finitely generated group with a fixed semigroup system S of generators (i.e. such that every element $g \in G$ can be expressed a product $g = s_1 \dots s_n$ for some $s_i \in S$). Let $\gamma_G^S(n)$ be the growth function of (G, S); recall that it is

$$\gamma_G^S(n) = \#\{g \in G |\, |g| \leq n\},$$

where $|g|$ is the minimal number of generators required to express g as a product.

The following observations are well-known:

Lemma 2.3. *Let G be a group and consider two finite generating sets S and T. Then $\gamma_G^S \sim \gamma_G^T$, with $\sim$ given in Definition 2.1.*

It is then meaningful to consider the *growth* γ_G of G, which is the $\sim$-equivalence class containing its growth functions γ_G^S.

Lemma 2.4. *Let G be a finitely generated group, $H < G$ a finitely generated subgroup and K a quotient of G. Then $\gamma_H \precsim \gamma_G$ and $\gamma_K \precsim \gamma_G$.*

Proof. Let S be a finite generating set for H; choose a generating set $T \supset S$ for G. Apply Definition 2.1 with $C = 1$ to obtain $\gamma_H^S \precsim \gamma_G^T$. Clearly $\gamma_K^T(n) \leq \gamma_G^T(n)$ for all n. □

Lemma 2.5 ([Gri89])**.** *For any field $\Bbbk$ and any group G with generating set S the inequalities $a_n(G) \leq \gamma_G^S(n)$ hold for all $n \geq 0$.*

Proof. Fix a generating set S. The identities

$$xy - 1 = (x-1) + (y-1) + (x-1)(y-1), \qquad x^{-1} - 1 = -(x-1) - (x-1)(x^{-1}-1)$$

show that

$$xy - 1 \equiv (x-1) + (y-1), \qquad x^{-1} - 1 \equiv -(x-1) \mod \Delta^2,$$

so Δ^n is generated over $\Bbbk$ by Δ^{n+1} and elements of the form

$$x_0(s_1 - 1)x_1(s_2 - 1)\dots(s_n - 1)x_n,$$

for all $s_i \in S$ and $x_i \in \Bbbk[G]$. Now $x_i \equiv \varepsilon(x_i) \in \Bbbk$ modulo Δ, so Δ^n/Δ^{n+1} is spanned by the

$$(s_1 - 1)(s_2 - 1)\dots(s_n - 1), \qquad s_i \in S.$$

All these elements are in the vector subspace S_n of $\Bbbk[G]$ spanned by products of at most n generators, and by definition S_n is of dimension $\gamma_G^S(n)$. □

Corollary 2.6. $\{a_n(G)\}_{n=0}^{\infty} \precsim \gamma_G$.

Combining Proposition 2.2 and Lemma 2.5, we obtain as

Corollary 2.7. *If there exist $C > 0$ and $d \geq 0$ such that $b_n \geq Cn^d$ for all n, then $\gamma_G(n) \succsim e^{1-1/(d+2)}$. In particular, if $b_n \neq 0$ for all n, then $\gamma_G(n) \succsim e^{\sqrt{n}}$.*

We shall say a group G is of *subradical growth* if $\gamma_G \precnsim e^{\sqrt{n}}$.

Theorem 2.8 ([Gri89])**.** *Let G be a finitely generated residually-p group. If G is of subradical growth then G is virtually nilpotent and $\gamma_G(n) \sim n^d$ for some $d \in \mathbb{N}$.*

Proof. By the previous corollary, $b_n(G) = 0$ for some n. Consider the p-completion $\widehat{G}$ of G. As Lie algebras, $\mathcal{L}_{\mathbb{F}_p}(G)$ and $\mathcal{L}_{\mathbb{F}_p}(\widehat{G})$ coincide, so $b_n(\widehat{G}) = 0$. By Lazard's criterion $\widehat{G}$ is an analytic pro-p-group [Laz65] and thus is linear over a field. Since G is residually-p it embeds in $\widehat{G}$ so is also linear. By the Tits alternative [Tit72] either G contains a free group on two generators (contradicting the assumption on the growth of G) or G is virtually solvable. By the results of Milnor and Wolf every virtually solvable group is either of exponential growth or is virtually nilpotent [Mil68, Wol68]. The asymptotic growth is invariant under taking finite-index subgroups, and the growth of a nilpotent group is polynomial of degree $\sum_{k\geq 1} kb_k$, as was shown by Guivarc'h and Bass [Gui70, Gui73, Bas72]. □

In the class of residually-p groups, Theorem 2.8 improves Gromov's result [Gro81a] that a finitely generated group G having polynomial growth is virtually nilpotent, in that the assumption is weakened from 'polynomial growth' to 'subradical growth'. Lubotzky and Mann have shown the same result for residually nilpotent groups of subradical growth. It is not known whether subradical growth does imply virtual nilpotence, and whether there exist groups of precisely radical growth. Certainly the right place to look for such examples is among groups of finite width, or groups satisfying some tight condition on the growth of their b_n.

Therefore new examples of groups of finite width are of special interest. Below we shall give two examples of such groups and outline a method of constructing new examples; but first a consequence of 2.8 is

Theorem 2.9. *The growth $\gamma_{\mathfrak{G}}$ of the group $\mathfrak{G}$ satisfies*

$$e^{\sqrt{n}} \precsim \gamma_{\mathfrak{G}}(n) \precsim e^{n^{1/(1-\log_2 \eta)}},$$

where η is the real root of $X^3 + X^2 + X - 2$.

Proof. If $\mathfrak{G}$ were nilpotent it would be finite, as it is finitely generated and torsion; since it is infinite 2.8 yields the left inequality.

The right inequality was proven by the first author in [Bar98], using purely combinatorial techniques. □

Note that the estimate from below can be obtained directly as in [Gri84], by showing that for an appropriate S the growth function γ_G^S satisfies

$$\gamma_G^S(4n) \geq \gamma_G^S(n)^2.$$

The second author conjectured in 1984 that the left inequality is in fact an equality, but Leonov recently announced that this is not the case [Leo98].

For our second example $\widetilde{\mathfrak{G}}$ it is only known that

$$e^{\sqrt{n}} \precsim \gamma_{\widetilde{\mathfrak{G}}} \precnsim e^n,$$

as is shown in [BG99].

Lemma 2.5 can also be used to study uniformly exponential growth, as was observed in [CG97]. Let

$$\omega_G^S = \lim_{n\to\infty} \sqrt[n]{\gamma_G^S(n)}$$

be the base of exponential growth of G with respect to the generating set S and let $\omega_G = \inf_S \omega_G^S$, the infimum being taken over all finite generating sets.

Definition 2.10. The group G has *uniformly exponential growth* if $\omega_G > 1$.

(See [Gro81b] for the original definition and motivations, and [GH97] for more details on this notion.) For instance, the free groups of rank ≥ 2, and more generally, the non-elementary hyperbolic groups have uniformly exponential growth [Kou98]. It is currently not known whether there exists a group of exponential but not uniformly exponential growth.

Corollary 2.11. *If for some $\Bbbk \in \{\mathbb{Q}, \mathbb{F}_p\}$ the algebra $\mathcal{A}_\Bbbk(G)$ has exponential growth then G has uniformly exponential growth. (We do not need here the assumption that G is residually-p or residually nilpotent.)*

In the next section we will combine this idea with the Golod-Shafarevich construction to produce examples of finitely generated residually finite p-groups of uniformly exponential growth.

3. Torsion Groups of Uniformly Exponential Growth

As a reference to the Golod-Shafarevich construction we recommend the original paper [GS64], one of the books [Her94, Koc70], or [HB82, § VIII.12].

Consider the free associative algebra A over the field $\mathbb{F}_p$ on the generators $x_1, \dots, x_d$ for some $d \geq 2$. The algebra A is graded: $A = \bigoplus_{n=0}^\infty A_n$ where A_n is spanned by the monomials of degree n, with $A_0 = \mathbb{F}_p 1$. Elements of the subspace A_n are called *homogeneous of degree n*.

Consider an ideal $\mathcal{I}$ in A generated by r_1 homogeneous elements of degree 1, r_2 of degree 2, etc. (We make this homogeneity assumption for simplicity; it is not necessary, as was indicated in [Koc70].) Let $B = A/\mathcal{I}$. Then B is also a graded algebra: $B = \bigoplus_{n=0}^\infty B_n$ and if $H_B(t) = \sum_{n=0}^\infty d_n t^n$ be the Hilbert-Poincaré series of B, i.e. $d_n = \dim_{\mathbb{F}_p} B_n$, then the Golod-Shafarevich inequality

$$H_B(t)(1 - dt + H_R(t)) \geq 1 \tag{4}$$

holds; here $H_R(t) = \sum_{n=1}^\infty r_n t^n$, and for the comparison of two power series the same agreement holds as in the previous section.

Suppose that for some $\xi \in (0,1)$ the series $H_R(t)$ converges at ξ and $1 - d\xi + H_R(\xi) \leq 0$. Then the series $H_B(t)$ cannot converge at $t = \xi$, so the coefficients d_n of $H_B(t)$ grow exponentially and

$$\limsup_{n\to\infty} \sqrt[n]{d_n} \geq \frac{1}{\xi}.$$

Golod proves in [Gol64] that $\mathcal{I}$ can be chosen in such a way that the ideal $\mathcal{D} = \bigoplus_{n=1}^{\infty} B_n$ will be a p-nilalgebra (i.e. for all $y \in \mathcal{D}$ there is an $n \in \mathbb{N}$ such that $y^{p^n} = 0$).

The construction of the relators goes as follows: enumerate first as $\{y_k\}_{k=1}^{\infty}$ all elements of the algebra A (this is possible since A is countable). Start with $\mathcal{I}_0 = 0$; then if y_k is not a nilelement of $A/\mathcal{I}_{k-1}$ take $\ell_k \geq 3$ sufficiently large so that the least degree of monomials in $y_k^{p^{\ell_k}}$ is larger than all degrees of monomials in $\mathcal{I}_{k-1}$. Construct $\mathcal{I}_k$ by adding to $\mathcal{I}_{k-1}$ all homogeneous parts of the polynomial $y_k^{p^{\ell_k}}$. Let finally $\mathcal{I} = \bigcup_{n=0}^{\infty} \mathcal{I}_n$.

The numbers r_k will then all be 0 or 1 with $r_k = 0$ for $k < p^3$, so taking $\xi = 3/4$ we have

$$1 - d\xi + H_R(\xi) \leq 1 - 2\xi + \frac{\xi^{2^3}}{1-\xi} < 0$$

and $B = A/\mathcal{I}$ is of exponential growth at least $(4/3)^n$. Let $\overline{x}_1, \dots, \overline{x}_d$ be the images of $x_1, \dots, x_d$ in B, and let G be the group generated by the elements $s_i = 1 + \overline{x}_i$; they are invertible because the $\overline{x}_i$ are p-nilelements and B is of characteristic p. The vector subspace of B spanned by G is B itself, so B is a quotient of the group algebra $\mathbb{F}_p[G]$.

Theorem 3.1. *G is a finitely generated residually finite p-group of uniformly exponential growth.*

Proof. That G is a p-group was observed by Golod and follows from the fact that $\mathcal{D} = \bigoplus_{n=1}^{\infty} B_n$ is a p-nilalgebra. Let π be the natural map $\mathbb{F}_p[G] \to B$. Then $\mathcal{D}$ is generated by $\pi(\Delta)$ and more generally $\bigoplus_{n=N}^{\infty} B_n = \pi(\Delta^N)$, so by Lemmata 2.5 and 2.4 there is a $\xi < 1$ such that the estimate

$$\frac{1}{\xi^n} \leq \dim_{\mathbb{F}_p} B_n \leq a_n(G) \leq \gamma_G^T(n), \qquad n = 1, 2, \dots$$

holds for any system T of generators of G. $\square$

4. Growth of Algebras and Amenability

As was mentioned in the introduction, there is an interesting question (due to Vershik) on the relation between the amenability of a group and the growth of related algebras. Let us formulate our version of this question:

Problem 4.1. 1. *Let G be amenable. Does $b_n(G)$ grow subexponentially for any field $\Bbbk$?*
2. *Suppose G is residually nilpotent (or residually-p) and $b_n(G)$ grows subexponentially for the field $\mathbb{Q}$ (or $\mathbb{F}_p$). Is then the group G amenable?*

There is a chance that for at least one of these questions the answer is affirmative.

For solvable groups (which are amenable) the associated algebras have subexponential growth, as follows from computations by Petrogradskiĭ [Pet93, Pet96]; his results are based on computations for free polynilpotent algebras by Bokut' [Bok63]. See also Egorychev [Ego84] and Bereznĭ [Ber83] for partial results.

On the other hand there is some similarity between the asymptotics of random walks on solvable groups and the growth of $b_n(G)$ [Kaĭ80] which gives a hope that subexponential growth of algebras implies (under the residuality hypothesis) subexponential decay of the probability of returning to the origin for symmetric random walks on a group. Then Kesten's criterion [Kes59] can be invoked to imply the amenability of G.

5. Groups Acting on Rooted Trees

We now consider examples of groups whose lower central series and dimension series we can compute explicitly. Let Σ be a finite alphabet, and Σ^* the set of finite sequences over Σ. This set has a natural rooted tree structure: the vertices are finite sequences, and the edges are all the $(\sigma, \sigma s)$ for $\sigma \in \Sigma^*$ and $s \in \Sigma$; the root vertex is $\emptyset$, the empty sequence. By $\mathsf{Aut}(\Sigma^*)$ we mean the bijections of Σ^* that preserve the tree structure, i.e. preserve length and prefixes. We write $\sigma\Sigma^*$ for the subtree of Σ^* below vertex σ: it is isomorphic to Σ^* but rooted at σ.

Let G be a finitely generated subgroup of $\mathsf{Aut}(\Sigma^*)$ acting transitively on Σ^n for all n (such an action will be called *spherically transitive.*) We denote by $\mathsf{Stab}_G(\sigma)$ the stabilizer of the vertex σ in G, and by $\mathsf{Stab}_G(n)$ the stabilizer of all vertices of length n. An arbitrary element $g \in \mathsf{Stab}_G(n)$ can be identified with a tuple $(g_\sigma)_{|\sigma|=n}$ of tree automorphisms; we write this monomorphism

$$\phi_n : \mathsf{Stab}_G(n) \hookrightarrow \prod_{\sigma\in\Sigma^n} \mathsf{Aut}(\sigma\Sigma^*).$$

We define the *vertex group* or *rigid stabilizer* $\mathsf{Rist}_G(\sigma)$ of the vertex σ by

$$\mathsf{Rist}_G(\sigma) = \{g \in G |\, g\tau = \tau \;\forall \tau \in \Sigma^* \setminus \sigma\Sigma^*\},$$

and the n^{th} *rigid stabilizer* as the group generated by the length-n vertex groups: $\mathsf{Rist}_G(n) = \langle \mathsf{Rist}_G(\sigma) : \, |\sigma| = n\rangle$. Since G acts transitively on Σ^n the vertex groups of vertices at level n are all conjugate. Therefore $\mathsf{Rist}_G(n)$ is a direct product of $|\Sigma|^n$ copies of $\mathsf{Rist}_G(\sigma)$ for a σ of length n.

Definition 5.1. A finitely generated group G is called a *branch group* if

1. G acts faithfully on Σ^* and transitively on Σ^n for all $n \geq 0$;
2. $[G : \mathsf{Rist}_G(n)]$ is finite for all $n \geq 0$.

5.1. **The Modules V_n.** Let G be a group acting on a regular rooted tree Σ^*, where Σ contains p elements for some prime p; for ease of notation suppose $\Sigma = \mathbb{F}_p$. Assume moreover that at each vertex G acts as a power of the cyclic permutation $\epsilon = (0, 1, \dots, p-1)$ of Σ. Let $V_n = \mathbb{F}_p[G/\mathsf{Stab}_G(0^n)]$; it is a vector space of dimension p^n, as G acts transitively on Σ^n, and has a natural G-module structure coming from the action of G on $G/\mathsf{Stab}_G(0^n)$. Identify $G/\mathsf{Stab}_G(0^n)$ with the set Σ^n of vertices at level n, and also with the set of monomials over $\{X_1, \dots, X_n\}$ of degree $< p$ in each variable, by

$$\sigma = \sigma_1 \dots \sigma_n \leftrightarrow X_1^{\sigma_1} \dots X_n^{\sigma_n}.$$

Under this identification, we can write

$$\begin{aligned} V_n &= \mathbb{F}_p[X_1, \dots, X_n]/(X_1^p - 1, \dots, X_n^p - 1) \\ &= \mathbb{F}_p[X_1]/(X_1^p - 1) \otimes \dots \otimes \mathbb{F}_p[X_n]/(X_n^p - 1). \end{aligned}$$

We write $g\sigma$ the action of $g \in G$ on $\sigma \in V_n$, and denote by $[g, \sigma] = \sigma - g\sigma$ the "Lie action" of G on V_n. For $r \in \{0, \dots, p^n - 1\}$ we write $r = r_n \dots r_1$ in base p, and define

$$v_n^r = (1 - X_1)^{r_1} \dots (1 - X_n)^{r_n} \in V_n,$$
$$V_n^r = \langle v_n^r, \dots, v_n^{p^n - 1} \rangle.$$

We extend the last definition to $V_n^r = 0$ when $r \geq p^n$. There is a natural projective sequence

$$\dots \to V_n \to V_{n-1} \to \dots \to V_0 = \mathbb{F}_p$$

of G-modules, and at each step n a sequence of V_n-submodules

$$V_n^{p^n} = 0 \subset \dots \subset V_n^{p^n - p^{n-1}} \subset \dots \subset V_n^1 \subset V_n^0 = V_n$$

each having codimension 1 in the next. Moreover $V_{n-1}^{p^{n-1} - i}$ and $V_n^{p^n - i}$ are naturally isomorphic under multiplication by $(1 - X_n)^{p-1}$; thus $V_n^{p^n - p^{n-1}}$ is isomorphic to $V_{n-1}^0 = V_{n-1}$ as a G-module.

Lemma 5.2. 1. *The inclusion $[G, V_n^r] \subset V_n^{r+1}$ holds for all n and all r.*
2. *If G contains for all $m \leq n$ an element g_m such that*

$$g_m(0^m) = 0^{m-1}1, \qquad g_m(\sigma x) = \sigma' x \quad \forall \sigma \in \Sigma^{m-1} \setminus \{0^{m-1}\}, x \in \Sigma$$

(where in the second condition σ' is an arbitrary function of σ), then $[G, V_n^r] = V_n^{r+1}$ for all n and all r.

A G-module V having the property $\dim V^{(n)}/V^{(n+1)} = 1$ for all n, where the $V^{(n)}$ are defined inductively by $V^{(0)} = V$ and $V^{(n+1)} = [G, V^{(n)}]$ is called *uniserial*. This notion was introduced by Leedham-Green [LG94]; see also [DdSMS91, page 111].

Note that every element of G can be described by a colouring $\{g_\sigma\}_{\sigma\in\Sigma^*}$ of the vertices of Σ^* by elements of the cyclic group $C_p = \langle\epsilon\rangle$. The condition in the lemma amounts to the existence, for all m, of an element g_m whose colouring is ϵ at the vertex 0^m, and is 1 on all other vertices of the m-th level as well as on all vertices 0^i, for $i < m$. Note also that this implies that the action is spherically transitive.

Proof. We proceed by induction on (n, r) in lexicographic order. For $n = 0$ the claim holds trivially; suppose thus $n \geq 1$. In order to prove $[G, V_n^r] \subset V_n^{r+1}$, it suffices to check that for all $g \in G$ we have $[g, v_n^r] \in V_n^{r+1}$, as the V_n^r form an ascending tower of subspaces. During the proof we will consider V_{n-1} as a subspace of V_n; beware though that it is not a submodule. We shall write '$*$' for the action of G on $V_{n-1} \subset V_n$, and '$\cdot$' for that of G on V_n.

Observe that if $v \in V_{n-1}$ then $g \cdot (vX_n^i) = (g \cdot v)X_n^i$. Thus $g \cdot v - g * v$ is always divisible by $1 - X_n$ because if $g \cdot v = \sum_{s=0}^{p-1} \Psi_s X_n^s$ for some $\Psi_s \in V_{n-1}$ then $g * v = \sum_{s=0}^{p-1} \Psi_s$ and

$$g \cdot v - g * v = (1 - X_n) \sum_{s=1}^{p-1} -\Psi_s(1 + X_n + \cdots + X_n^{s-1}). \tag{5}$$

Write $r = r_n \dots r_1$ in base p. For some Φ and Ψ_s in V_{n-1}, we may write

$$v_n^r = \Phi(1 - X_n)^{r_n}, \qquad g \cdot v_n^r = \sum_{s=0}^{p-1} \Psi_s X_n^s (1 - X_n)^{r_n}.$$

Then by induction

$$[g, v_n^r] = \underbrace{\underbrace{\left(\Phi - \sum_{s=0}^{p-1} \Psi_s\right)}_{\in V_{n-1}^{(r+1) \bmod p^{n-1}}} (1 - X_n)^{r_n}}_{\in V_n^{r+1}} + \underbrace{\sum_{s=0}^{p-1} \Psi_s (1 - X_n^s)(1 - X_n)^{r_n}}_{\in V_n^{(r_n+1)p^{n-1}} \subseteq V_n^{r+1}},$$

as in the second summand $(1 - X_n^s)(1 - X_n)^{r_n}$ is divisible by $(1 - X_n)^{r_n+1}$. This proves the first claim of the lemma.

Next, we prove $[G, V_n^r] \supset V_n^{r+1}$ by showing that $v_n^{r+1} \in [G, V_n^r]$. As above, write $r = r_n \dots r_1$ in base p. If $(r_1, \dots, r_{n-1}) \neq (p-1, \dots, p-1)$, we have $v_n^{r+1} = v_{n-1}^{r+1 \bmod p^{n-1}}(1 - X_n)^{r_n}$, and by induction $v_{n-1}^{r+1 \bmod p^{n-1}} = \sum_s \alpha_s [g_s, v_{n-1}^{i_s}]$ for some $\alpha_s \in \mathbb{F}_p$, $g_s \in G$ and $i_s \geq r \bmod p^{n-1}$. Then

$$v_n^{r+1} = \underbrace{\sum_s \alpha_s \left[g_s, v_n^{i_s + r_n p^{n-1}}\right]}_{\in [G, V_n^r]} + \underbrace{\sum_s \alpha_s \left(g_s \cdot v_n^{i_s + r_n p^{n-1}} - (g_s * v_{n-1}^{i_s})(1 - X_n)^{r_n}\right)}_{\in V_n^{(r_n+1)p^{n-1}} \subseteq V_n^{r+2} \subseteq [G, V_n^{r+1}] \subseteq [G, V_n^r]}$$

where the last inclusions hold by (5) and induction. Finally, if $r = (r_n + 1)p^{n-1} - 1$, note that

$$\begin{aligned} v_n^r &= (1 + X_1 + \cdots + X_1^{p-1}) \cdots (1 + X_{n-1} + \cdots + X_{n-1}^{p-1})(1 - X_n)^{r_n} \\ &= (1 - X_n)^{r_n} + P(1 - X_n)^{r_n}, \end{aligned}$$

where $P = \sum_{\sigma \in \Sigma^{n-1} \setminus \{0^{n-1}\}} X_1^{\sigma_1} \cdots X_n^{\sigma_n}$ is invariant under g_n; thus

$$v_n^{r+1} = (1 - X_n)^{r_n} - X_n(1 - X_n)^{r_n} = [g_n, v_n^r] \in [G, V_n^r].$$

□

The strategy we follow to compute the lower central series or dimension series of G in the examples of Sections 6 and 7 is the following:

- We recognize some $\gamma_m(G)$ or G_m as a subgroup of G simply obtained from rigid stabilizers in G.
- We identify a quotient $\gamma_m(G)/N$ or G_m/N with a direct sum of copies of the module V_n defined above, for an appropriate subgroup N.
- We show that N is a further term of the lower central or dimensional series, allowing the process to repeat.

Then the exact terms of the lower central or dimension series are obtained by pulling back the appropriate V_n^r through the identification.

6. The Group $\mathfrak{G}$

Let $\Sigma = \mathbb{F}_2$, the field on two elements. For $x \in \mathbb{F}_2$ set $\overline{x} = 1 - x$, and define the automorphisms a, b, c, d of Σ^* as follows:

$$a(x\sigma) = \overline{x}\sigma,$$

$$\begin{aligned} b(0x\sigma) &= 0\overline{x}\sigma, & b(1\sigma) &= 1c(\sigma), \\ c(0x\sigma) &= 0\overline{x}\sigma, & c(1\sigma) &= 1d(\sigma), \\ d(0x\sigma) &= 0x\sigma, & d(1\sigma) &= 1b(\sigma). \end{aligned}$$

Thus for instance b acts on the subtree $0\Sigma^*$ as c, while c acts on it as d, etc. Note that all generators are of order 2 and $\{1, b, c, d\}$ forms a Klein group. Set $\mathfrak{G} = \langle a, b, c, d \rangle$. For ease of notation, we shall identify elements of $\mathsf{Stab}_{\mathfrak{G}}(n)$ with their image under ϕ_n by writing $\phi_n(g) = (g_1, \dots, g_{2^n})_n$ (omitting the subscript n if it is obvious from context); for instance we will write $b = (a, c)$, $c = (a, d)$ and $d = (1, b)$. Set $x = [a, b]$, and set

$$K = \langle x \rangle^{\mathfrak{G}} = \langle x, (x, 1), (1, x) \rangle.$$

Note that $(x, 1) = [b, d^a]$ and $(1, x) = [b^a, d]$. Also, K is a subgroup of finite index (actually index 16) in $\mathfrak{G}$, and contains $K \times K$ as a subgroup of finite index (actually index 4); for more details see [Har00] or [BG99]. Set also $T = \langle x^2 \rangle^{\mathfrak{G}} = K^2$, and for any $Q \le K$ define $Q_m = Q \times \cdots \times Q$ (2^m copies). Clearly $Q_m \le \mathsf{Stab}_{\mathfrak{G}}(m)$ and acts on each subtree starting on level m by the corresponding factor. For $m \ge 1$ set $N_m = K_m \cdot T_{m-1}$.

For $m \geq 2$, we have $\mathsf{Rist}_{\mathfrak{G}}(m) = K_{m-2}$, so $\mathfrak{G}$ is a branch group.

Lemma 6.1. *The mapping*

$$\alpha \oplus \beta : N_m/N_{m+1} \longrightarrow V_m \oplus V_{m-1}$$

is an isomorphism for all m, where the V_m are the modules defined in Subsection 5.1, α maps $(1, \dots, 1, x, 1, \dots, 1) \in K_m$ to the monomial in V_m corresponding to the vertex at the x's position, and β maps $(1, \dots, 1, x^2, 1, \dots, 1) \in T_{m-1}$ to the corresponding monomial in V_{m-1}.

Proof. We first suppose $m = 1$. Then $N_1/N_2 = \langle x^2, (1, x), (x, 1)\rangle/N_2$; it is easy to check that $x^4 = (x^2, x^2)$ modulo K_2, so all generators of N_1/N_2 are of order 2. Further, $[x^2, (1, x)] \in K_2$ and $[x^2, (x, 1)] \in K_2$, so the quotient N_1/N_2 is the elementary abelian group 2^3, and $\alpha \oplus \beta$ is an isomorphism in that case.

For $m > 1$ it suffices to note that both sides of the isomorphism are direct sums of 2^{m-1} terms on each of which the lemma for $m = 1$ can be applied. □

Lemma 6.2. *The following equalities hold in $\mathfrak{G}$:*

$$\begin{aligned} [x, a] &= x^2, & [x, b] &= x^2, \\ [x, c] &= x(1, x^{-1})x, & [x, d] &= (1, x), \\ [x^2, a] &= x^4 = ((U, V)x^2, (V, U)x^2), & [x^2, b] &= x^4, \\ [x^2, c] &= ((U, V)x^2, (1, x)), & [x^2, d] &= (1, (U, 1)x^2), \end{aligned}$$

where $U = (1, x^{-1})x$ and $V = (x^{-1}, 1)x^{-1}$ are in K.

Proof. Direct computation; see also [Roz96b], where different notations are used. □

Lemma 6.3. *If $Q \gneqq N_{m+1}$ contains $g = (x, \dots, x) \in K_m$, then $[Q, \mathfrak{G}] \geq N_{m+1}$.*

Proof. Let $b_m \in \{b, c, d\}$ be such that it acts like b on $1^m\Sigma^*$. Then

$$h = [g, b_m] = (1, \dots, 1, [x, b])_m = (1, \dots, 1, x^2)_m \in T_m.$$

Conjugating h by elements of g yields all cyclic permutations of the above vector, so as $[G, \mathfrak{G}]$ is normal in G it contains T_m. Likewise, let d_m act like d on $1^m\Sigma^*$. Then

$$[g, d_m] = (1, \dots, 1, [x, a], [x, d])_m = (1, \dots, 1, x^2, (1, x))_m;$$

using $T_m \leq [Q, \mathfrak{G}]$, we obtain $(1, \dots, 1, (1, x))_m = (1, \dots, 1, x)_{m+1} \in [Q, \mathfrak{G}]$, so by the same conjugation argument $[Q, \mathfrak{G}] \geq K_{m+1}$. □

Theorem 6.4. *For all $m \geq 1$ we have:*

1. $\gamma_{2^m+1}(\mathfrak{G}) = N_m$.
2. $\gamma_{2^m+1+r}(\mathfrak{G}) = N_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_{m-1}^r)$ *for* $r = 0, \ldots, 2^m$.
3.

$$\operatorname{rank}(\gamma_n(\mathfrak{G})/\gamma_{n+1}(\mathfrak{G})) = \begin{cases} 3 & \text{if } n = 1, \\ 2 & \text{if } n = 2, \\ 2 & \text{if } n = 2^m + 1 + r, \text{ with } 0 \leq r < 2^{m-1}, \\ 1 & \text{if } n = 2^m + 1 + r, \text{ with } 2^{m-1} \leq r \leq 2^m. \end{cases}$$

Proof. First compute $\gamma_2(\mathfrak{G}) = \mathfrak{G}' = \langle [a,d], K \rangle$; it is of index 8 in $\mathfrak{G}$, with quotient generated by $\{a,b,c\}$. Compute also $\gamma_3(\mathfrak{G}) = \langle x^2 = [x,a], (1,x) = [x,d] \rangle^{\mathfrak{G}} = N_1$ of index 2 in $\gamma_2(\mathfrak{G})$, with quotient generated by $\{x^2, (1,x)\}$. This gives the basis of an induction on $m \geq 1$ and $0 < r \leq 2^m$.

Assume that $\gamma_{2^m+1}(\mathfrak{G}) = N_m$. Note that the hypothesis of Lemma 5.2 is satisfied; indeed g_m can even be chosen among the conjugates of b, c or d. Consider the sequence of quotients $Q_r = N_{m+1}\gamma_{2^m+1+r}(\mathfrak{G})/N_{m+1}$ for $r \geq 0$. Lemmata 6.1 and 5.2 tell us that $Q_r = \alpha^{-1}(V_m^r) \oplus \beta^{-1}(V_{m-1}^r)$; in particular $Q_r \ni (x, \ldots, x) = \alpha^{-1}(v_m^{2^m-1})$ for all $r < 2^m$, and then Lemma 6.3 tells us that $\gamma_{2^m+1+r}(\mathfrak{G}) \geq N_{m+1}$ for $r \leq 2^m$. When $r = 2^m$ we have $\gamma_{2^{m+1}+1}(\mathfrak{G}) = N_{m+1}$ and the induction can continue. □

Lemma 6.5. *For all $m \geq 1$ and $r \in \{0, \ldots, 2^m - 1\}$ we have:*

$$(\alpha^{-1}V_m^r)^2 = \beta^{-1}(V_m^r) \leq N_{m+1};$$
$$(\beta^{-1}V_{m-1}^r)^2 = \beta^{-1}(V_m^{r+2^{m-1}}) \leq N_{m+1}.$$

Proof. Write $\alpha^{-1}(v_m^r) = (x^{i_1}, \ldots, x^{i_{2^m}})$ or $\beta^{-1}(v_m^r) = (x^{2i_1}, \ldots, x^{2i_{2^m}})$ for some $i_* \in \{0,1\}$. Then these claims follow immediately, using Lemma 6.2, from

$$\begin{aligned} (\alpha^{-1}v_m^r)^2 &= (x^{i_1}, \ldots, x^{i_{2^m}})^2 = (x^{2i_1}, \ldots, x^{2i_{2^m}}) = \beta^{-1}(v_m^r), \\ (\beta^{-1}v_{m-1}^r)^2 &= (x^{2i_1}, \ldots, x^{2i_{2^{m-1}}})^2 = (x^{4i_1}, \ldots, x^{4i_{2^{m-1}}}) \\ &\equiv (x^{2i_1}, x^{2i_1}, \ldots, x^{2i_{2^{m-1}}}, x^{2i_{2^{m-1}}}) = \beta^{-1}(v_m^{r+2^{m-1}}) \mod N_{m+1}. \end{aligned}$$

□

Theorem 6.6. *For all $m \geq 1$ we have:*

1. $\mathfrak{G}_{2^m+1} = N_m$.
2.

$$\mathfrak{G}_{2^m+1+r} = \begin{cases} N_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_{m-1}^{r/2}) & \text{if } 0 \leq r \leq 2^m \text{ is even}, \\ N_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_{m-1}^{(r-1)/2}) & \text{if } 0 \leq r \leq 2^m \text{ is odd}. \end{cases}$$

3.

$$\operatorname{rank}(\mathfrak{G}_i/\mathfrak{G}_{i+1}) = \begin{cases} 3 & \text{if } i = 1, \\ 2 & \text{if } i > 1 \text{ is even}, \\ 1 & \text{if } i > 1 \text{ is odd}. \end{cases}$$

Proof. First compute $\mathfrak{G}_2 = \gamma_2(\mathfrak{G})$ and $\mathfrak{G}_3 = \gamma_3(\mathfrak{G}) = N_1$. This gives the basis of an induction on $m \geq 1$ and $0 \leq r \leq 2^m$. Assume $\mathfrak{G}_{2^m+1} = N_m$. Consider the sequence of quotients $Q_{m,r} = N_{m+1}\mathfrak{G}_{2^m+1+r}/N_{m+1}$ for $r \geq 0$. We have $Q_{m,r} = [\mathfrak{G}, Q_{m,r-1}]Q^2_{m-1,\lfloor r/2 \rfloor}$ by (2). Lemmata 6.1, 6.5 and 5.2 tell us that $Q_r = \alpha^{-1}(V_m^r) \oplus \beta^{-1}(V_{m-1}^{\lfloor r/2 \rfloor})$; in particular $Q_r \ni (x, \dots, x) = \alpha^{-1}(v_m^{2^m-1})$ for all $r < 2^m$, and then Lemma 6.3 tells us that $\mathfrak{G}_{2^m+1+r} \geq N_{m+1}$ for $r \leq 2^m$. When $r = 2^m$ we have $\mathfrak{G}_{2^{m+1}+1} = N_{m+1}$ and the induction can continue. □

6.1. **Cayley graphs of Lie algebras.** We introduce the notion of *Cayley graph* for graded Lie algebras. Let $L = \bigoplus_{n=1}^{\infty} L_n$ be a graded Lie algebra generated by a finite set S of degree one elements. Fix a basis $(\ell_{n,1}, \dots, \ell_{n,\dim L_n})$ of L_n for every n, and give each L_n an orthogonal scalar product $\langle \ell_{n,i} | \ell_{n,j} \rangle = \delta_{i,j}$. The *Cayley graph* of L is defined as follows: its vertices are the $(i,j) \in \mathbb{N}^2$ with $i \geq 1$ and $1 \leq j \leq \dim L_n$. For every $s \in S$ and $i, j, k \in \mathbb{N}$ there is an edge from (i,j) to $(i+1,k)$ labeled by s and with weight $\langle [\ell_{i,j}, s] | \ell_{i+1,k} \rangle$. By convention edges of weight 0 are not represented. Additionally, if L is a p-algebra, there is an unlabeled edge of length $(p-1)i$ from (i,j) to (pi,k) with weight $\langle \ell_{i,j}^p | \ell_{pi,k} \rangle$.

Clearly, the Cayley graph of a Lie algebra L determines the structure of L. It is a connected graph, because S is a generating set. The geometric growth of the graph is the same as the growth of the algebra.

As a simple example, consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ generated by $\{i, j\}$, and its dimension series $Q_1 = Q$, $Q_2 = \{\pm 1\}$ and $Q_3 = 1$ over the field $\mathbb{F}_2$. Then the Cayley graph of $\mathcal{L}(Q)$ is

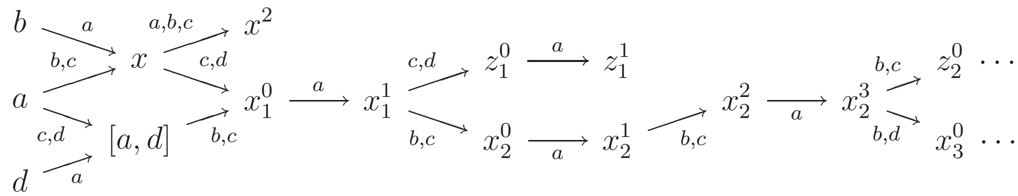
$$\begin{tikzcd} i \arrow[dr, "j"] & \\ & -1 \\ j \arrow[ur, "i"'] & \end{tikzcd}$$

We now describe the Cayley graphs of L and $\mathcal{L}_{\mathbb{F}_2}$ associated respectively to the lower central and dimensional series of $\mathfrak{G}$. Fix $S = \{a, b, c, d\}$ as a generating set for $\mathfrak{G}$, and extend it to $\overline{S} = \{a, b, c, d, \{ {}^b_c \}, \{ {}^b_d \}, \{ {}^c_d \}\}$. Define the transformation σ on $\overline{S}^*$ by

$$\sigma(a) = a\{ {}^b_c \}a, \quad \sigma(b) = d, \sigma(c) = b, \sigma(d) = b,$$

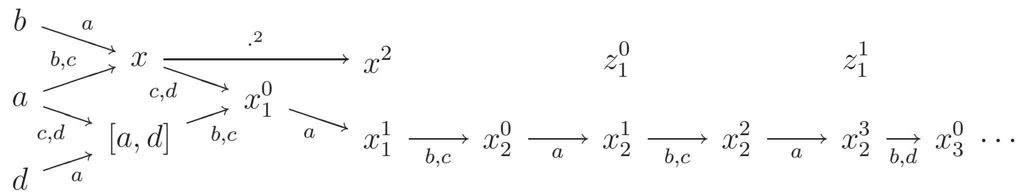
naturally extended to subsets. (For any fixed $g \in G$, one may obtain all elements $h \in \mathsf{Stab}_{\mathfrak{G}}(1)$ with $\phi(h) = (g, *)$ by computing $\sigma(g)$ and making all possible choices of a letter from the braced symbols. This explains the definition of $\overline{S}$.)

Theorem 6.7. *The Cayley graph of* $L(\mathfrak{G})$ *is as follows:*



where $x_m^r = \alpha^{-1}(v_m^r)$ *and* $z_m^r = \beta^{-1}(v_m^r)$. *The edge* $(x_m^{2^m-1}, x_{m+1}^0)$ *is labelled by* $\sigma^m\{\begin{smallmatrix} c \\ d \end{smallmatrix}\}$, *the edge* $(x_m^{2^m-1}, z_m^0)$ *is labelled by* $\sigma^m\{\begin{smallmatrix} b \\ d \end{smallmatrix}\}$, *and the paths from* x_m^0 *to* $x_m^{2^m-1}$ *and from* z_m^0 *to* $z_m^{2^m-1}$ *are labelled by* $\sigma^{m-1}(a)$.

The Cayley graph of $\mathcal{L}_{\mathbb{F}_2}(\mathfrak{G})$ *is as follows:*



with the same rule for labellings as for $L(\mathfrak{G})$; *and power maps from* x_m^r *to* z_m^r.

Note that as we are in characteristic 2 the non-zero weights can only be 1 and thus are not indicated.

7. The Group $\widetilde{\mathfrak{G}}$

We describe here the lower central and dimension series for a group $\widetilde{\mathfrak{G}}$ containing the previous section's group $\mathfrak{G}$ as a subgroup. More details about $\widetilde{\mathfrak{G}}$ can be found in [BG99].

As in Section 6 set $\Sigma = \mathbb{F}_2$, and define automorphisms $\tilde{b}$, $\tilde{c}$ and $\tilde{d}$ of Σ^* by

$$\begin{aligned} \tilde{b}(0x\sigma) &= 0\overline{x}\sigma, & \tilde{b}(1\sigma) &= 1\tilde{c}(\sigma), \\ \tilde{c}(0\sigma) &= 0\sigma, & \tilde{c}(1\sigma) &= 1\tilde{d}(\sigma), \\ \tilde{d}(0\sigma) &= 0\sigma, & \tilde{d}(1\sigma) &= 1\tilde{b}(\sigma). \end{aligned}$$

Note that all generators are of order 2 and $\{\tilde{b}, \tilde{c}, \tilde{d}\}$ generate the elementary abelian group 2^3. Set $\widetilde{\mathfrak{G}} = \langle a, \tilde{b}, \tilde{c}, \tilde{d}\rangle$. Clearly, $\mathfrak{G} = \langle a, b = \tilde{b}\tilde{c}, c = \tilde{c}\tilde{d}, d = \tilde{d}\tilde{b}\rangle$ is a subgroup of $\widetilde{\mathfrak{G}}$. Its index is infinite, because $\mathfrak{G}$ is a torsion group while $w = a\tilde{b}\tilde{c}\tilde{d}$ has infinite order, because $w^2 = (w^a, w)$. Set $x = [a, \tilde{b}]$, $y = [a, \tilde{d}]$, and

$$\tilde{K} = \langle x, y\rangle^{\widetilde{\mathfrak{G}}}.$$

Then $\tilde{K}$ is a subgroup of finite index (actually index 32) in $\mathfrak{G}$, and contains $\tilde{K} \times \tilde{K}$ as a subgroup of finite index (actually index 8). Set also $\tilde{T} = \langle x^2\rangle^{\mathfrak{G}} = \tilde{K}^2$, and for any $Q \le \tilde{K}$ define $Q_m = Q \times \cdots \times Q$ (2^m copies). For $m \ge 1$ set $\tilde{N}_m = \tilde{K}_m \cdot \tilde{T}_{m-1}$.

For $m \geq 2$, we have $\mathsf{Rist}_{\widetilde{\mathfrak{G}}}(m) = \tilde{K}_{m-2}$, so $\widetilde{\mathfrak{G}}$ is a branch group.

Lemma 7.1. *The mapping*

$$\alpha \oplus \beta \oplus \gamma : \tilde{N}_m/\tilde{N}_{m+1} \longrightarrow V_m \oplus V_m \oplus V_{m-1}$$

is an isomorphism for all m, where the V_m are the modules defined in Subsection 5.1, α maps $(1, \dots, x, \dots, 1) \in \tilde{K}_m$ to the monomial in V_m corresponding to the vertex in x's position, and β maps $(1, \dots, y, \dots, 1) \in \tilde{K}_m$ to the corresponding vertex in V_m, and γ maps $(1, \dots, x^2, \dots, 1) \in \tilde{T}_{m-1}$ to the corresponding monomial in V_{m-1}.

Proof. We first suppose $m = 1$. Then

$$\tilde{N}_1/\tilde{N}_2 = \langle x^2, (1, x), (x, 1), (1, y), (y, 1)\rangle/\tilde{N}_2;$$

it is easy to check that $x^4 = 1$, so all generators of $\tilde{N}_1/\tilde{N}_2$ are of order 2. Further, all commutators of generators belong to $\tilde{K}_2$, so the quotient $\tilde{N}_1/\tilde{N}_2$ is the elementary abelian group 2^5, and $\alpha \oplus \beta \oplus \gamma$ is an isomorphism in that case.

For $m > 1$ it suffices to note that both sides of the isomorphism are direct sums of 2^{m-1} terms on each of which the lemma for $m = 1$ can be applied. $\square$

Lemma 7.2. *The following equalities hold in $\widetilde{\mathfrak{G}}$:*

$$\begin{aligned}
[x, a] &= x^2, & [x, \tilde{b}] &= x^2 \\
[x, \tilde{c}] &= (1, y), & [x, \tilde{d}] &= (1, x), \\
[x^2, a] &= 1, & [x^2, \tilde{b}] &= 1, \\
[x^2, \tilde{c}] &= 1, & [x^2, \tilde{d}] &= (1, x(x, 1)x), \\
[y, a] &= 1, & [y, \tilde{b}] &= (x^{-1}, 1), \\
[y, \tilde{c}] &= 1, & [y, \tilde{d}] &= 1.
\end{aligned}$$

Proof. Direct computation. $\square$

Lemma 7.3. *If $Q \gneqq \tilde{N}_{m+1}$ contains $g = (x, \dots, x) \in \tilde{K}_m$, then $[Q, \widetilde{\mathfrak{G}}] \geq \tilde{N}_{m+1}$.*

Proof. Let $\tilde{b}_m \in \{\tilde{b}, \tilde{c}, \tilde{d}\}$ be such that it acts like $\tilde{b}$ on $1^m\Sigma^*$. Then

$$[g, \tilde{b}_m] = (1, \dots, 1, [x, \tilde{b}])_m = (1, \dots, 1, x^2)_m \in \tilde{T}_m,$$

so by a conjugation argument $[Q, \widetilde{\mathfrak{G}}] \geq \tilde{T}_m$. Likewise, let $\tilde{c}_m$ and $\tilde{d}_m$ act like c and d on $1^m\Sigma^*$. Then

$$\begin{aligned}
[g, \tilde{c}_m] &= (1, \dots, 1, [x, a], [x, \tilde{c}])_m = (1, \dots, 1, x^2, (1, y))_m, \\
[g, \tilde{d}_m] &= (1, \dots, 1, (1, x))_m.
\end{aligned}$$

Using $\tilde{T}_m \leq [Q, \widetilde{\mathfrak{G}}]$, we obtain $(1,\dots,1,(1,y))_m = (1,\dots,1,y)_{m+1} \in [Q,\widetilde{\mathfrak{G}}]$, so again by a conjugation argument $[Q,\widetilde{\mathfrak{G}}] \geq \tilde{K}_{m+1}$. $\square$

Theorem 7.4. *For all $m \geq 1$ we have:*

1. $\gamma_{2^m+1}(\widetilde{\mathfrak{G}}) = \tilde{N}_m$.
2. $\gamma_{2^m+1+r}(\widetilde{\mathfrak{G}}) = \tilde{N}_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_m^r)\gamma^{-1}(V_{m-1}^r)$ *for* $r = 0,\dots,2^m$.
3. $$\operatorname{rank}(\gamma_n(\widetilde{\mathfrak{G}})/\gamma_{n+1}(\widetilde{\mathfrak{G}})) = \begin{cases} 4 & \text{if } n = 1, \\ 3 & \text{if } n = 2, \\ 3 & \text{if } n = 2^m+1+r, \text{ with } 0 \leq r < 2^{m-1}, \\ 2 & \text{if } n = 2^m+1+r, \text{ with } 2^{m-1} \leq r \leq 2^m. \end{cases}$$

Proof. First compute $\gamma_2(\widetilde{\mathfrak{G}}) = \widetilde{\mathfrak{G}}' = \langle [a,\tilde{c}], \tilde{K}\rangle$, of index 16 in $\widetilde{\mathfrak{G}}$, and $\gamma_3(\widetilde{\mathfrak{G}}) = \langle x^2, (1,x), (1,y)\rangle^{\widetilde{\mathfrak{G}}} = \tilde{N}_1$, with $x^2 = [x,a]$, $(1,x) = [x,\tilde{d}]$ and $(1,y) = [x,\tilde{c}]$. This gives the basis of an induction on $m \geq 1$ and $0 \leq r \leq 2^m$.

Assume that $\gamma_{2^m+1}(\widetilde{\mathfrak{G}}) = \tilde{N}_m$. Note that the hypothesis of Lemma 5.2 is satisfied for $\widetilde{\mathfrak{G}}$, as it holds for $\mathfrak{G} < \widetilde{\mathfrak{G}}$. Consider the sequence of quotients $Q_r = \tilde{N}_{m+1}\gamma_{2^m+1+r}(\widetilde{\mathfrak{G}})/\tilde{N}_{m+1}$ for $r \geq 0$. Lemmata 7.1 and 5.2 tell us that $Q_r = \alpha^{-1}(V_m^r) \oplus \beta^{-1}(V_m^r) \oplus \gamma^{-1}(V_{m-1}^r)$; in particular $Q_r \ni (x,\dots,x) = \alpha^{-1}(v_m^{2^m-1})$ for all $r < 2^m$, and then Lemma 7.3 tells us that $\gamma_{2^m+1+r}(\widetilde{\mathfrak{G}}) \geq \tilde{N}_{m+1}$ for $r \leq 2^m$. When $r = 2^m$ we have $\gamma_{2^{m+1}+1}(\widetilde{\mathfrak{G}}) = \tilde{N}_{m+1}$ and the induction can continue. $\square$

Lemma 7.5. *For all $m \geq 1$ and $r \in \{0,\dots,2^m-1\}$ we have:*

$$(\alpha^{-1}V_m^r)^2 = \gamma^{-1}(V_m^r) \leq \tilde{N}_{m+1};$$
$$(\beta^{-1}V_m^r)^2 = 1 \leq \tilde{N}_{m+1};$$
$$(\gamma^{-1}V_{m-1}^r)^2 = \gamma^{-1}(V_m^{r+2^{m-1}}) \leq \tilde{N}_{m+1}.$$

Proof. Write $\alpha^{-1}(v_m^r) = (x^{i_1},\dots,x^{i_{2^m}})$, $\beta^{-1}(v_m^r) = (y^{i_1},\dots,y^{i_{2^m}})$ or $\gamma^{-1}(v_m^r) = (x^{2i_1},\dots,x^{2i_{2^m}})$ for some $i_* \in \{0,1\}$. Then these claims follow immediately, using Lemma 7.2, from

$$\begin{aligned}
(\alpha^{-1}v_m^r)^2 &= (x^{i_1},\dots,x^{i_{2^m}})^2 = (x^{2i_1},\dots,x^{2i_{2^m}}) = \gamma^{-1}(v_m^r), \\
(\beta^{-1}v_m^r)^2 &= (y^{i_1},\dots,y^{i_{2^m}})^2 = (y^{2i_1},\dots,y^{2i_{2^m}}) = (1,\dots,1), \\
(\gamma^{-1}v_{m-1}^r)^2 &= (x^{2i_1},\dots,x^{2i_{2^{m-1}}})^2 = (x^{4i_1},\dots,x^{4i_{2^{m-1}}}) \\
&\equiv (x^{2i_1},x^{2i_1},\dots,x^{2i_{2^{m-1}}},x^{2i_{2^{m-1}}}) = \gamma^{-1}(v_m^{r+2^{m-1}}) \mod \tilde{N}_{m+1}.
\end{aligned}$$

$\square$

Theorem 7.6. *For all $m \geq 1$ we have:*

1. $\widetilde{\mathfrak{G}}_{2^m+1} = \tilde{N}_m$.

2.

$$\widetilde{\mathfrak{G}}_{2^m+1+r} = \begin{cases} \tilde{N}_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_m^r)\gamma^{-1}(V_{m-1}^{r/2}) & \text{if } 0 \le r \le 2^m \text{ is even,} \\ \tilde{N}_{m+1}\alpha^{-1}(V_m^r)\beta^{-1}(V_m^r)\gamma^{-1}(V_{m-1}^{(r-1)/2}) & \text{if } 0 \le r \le 2^m \text{ is odd.} \end{cases}$$

3.

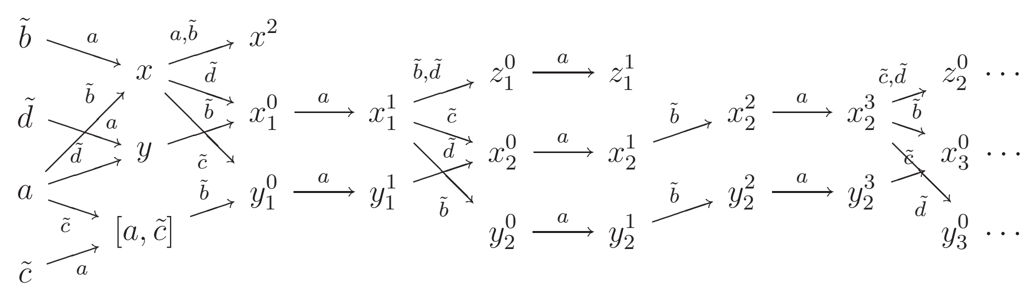
$$\operatorname{rank}(\widetilde{\mathfrak{G}}_i/\widetilde{\mathfrak{G}}_{i+1}) = \begin{cases} 4 & \text{if } i = 1, \\ 3 & \text{if } i > 1 \text{ is even,} \\ 2 & \text{if } i > 1 \text{ is odd.} \end{cases}$$

Proof. First compute $\widetilde{\mathfrak{G}}_2 = \gamma_2(\widetilde{\mathfrak{G}})$ and $\widetilde{\mathfrak{G}}_3 = \gamma_3(\widetilde{\mathfrak{G}}) = \tilde{N}_1$. This gives the basis of an induction on $m \ge 1$ and $0 \le r \le 2^m$. Assume $\mathfrak{G}_{2^m+1} = \tilde{N}_m$. Consider the sequence of quotients $Q_{m,r} = \tilde{N}_{m+1}\widetilde{\mathfrak{G}}_{2^m+1+r}/\tilde{N}_{m+1}$ for $r \ge 0$. We have $Q_{m,r} = [\widetilde{\mathfrak{G}}, Q_{m,r-1}]Q^2_{m-1,\lfloor r/2 \rfloor}$ by (2). Lemmata 7.1, 7.5 and 5.2 tell us that $Q_r = \alpha^{-1}(V_m^r) \oplus \beta^{-1}(V_m^r) \oplus \gamma^{-1}(V_{m-1}^{\lfloor r/2 \rfloor})$; in particular $Q_r \ni (x, \dots, x) = \alpha^{-1}(v_m^{2^m-1})$ for all $r < 2^m$, and then Lemma 7.3 tells us that $\mathfrak{G}_{2^m+1+r} \ge \tilde{N}_{m+1}$ for $r \le 2^m$. When $r = 2^m$ we have $\mathfrak{G}_{2^{m+1}+1} = \tilde{N}_{m+1}$ and the induction can continue. □

7.1. **The Lie Algebra Structures.** We describe here the Cayley graphs of L and $\mathcal{L}_{\mathbb{F}_p}$ associated respectively to the lower central and dimension series of $\widetilde{\mathfrak{G}}$. Consider $\tilde{S} = \{a, \tilde{b}, \tilde{c}, \tilde{d}\}$ and define the transformation $\tilde{\sigma}$ on $\tilde{S}^*$ by

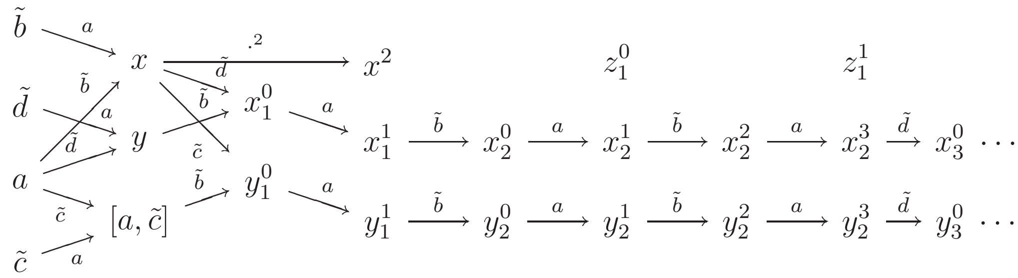
$$\tilde{\sigma}(a) = a\tilde{b}a, \quad \tilde{\sigma}(\tilde{b}) = \tilde{d}, \quad \tilde{\sigma}(\tilde{c}) = \tilde{b}, \quad \tilde{\sigma}(\tilde{d}) = \tilde{b}.$$

Theorem 7.7. *The Cayley graph of $L(\widetilde{\mathfrak{G}})$ is as follows:*



where $x_m^r = \alpha^{-1}(v_m^r)$, $y_m^r = \beta^{-1}(v_m^r)$ and $z_m^r = \gamma^{-1}(v_m^r)$. The edge $(x_m^{2^m-1}, x_{m+1}^0)$ is labelled by $\tilde{\sigma}^m(\tilde{d})$, the edges $(x_m^{2^m-1}, y_{m+1}^0)$ and $(x_m^{2^m-1}, z_m^0)$ are labelled by $\tilde{\sigma}^m(\tilde{b})$, the edges $(x_m^{2^m-1}, z_m^0)$ and $(y_m^{2^m-1}, x_{m+1}^0)$ are labelled by $\tilde{\sigma}^m(\tilde{c})$, and the paths from x_m^0 to $x_m^{2^m-1}$, from y_m^0 to $y_m^{2^m-1}$ and from z_m^0 to $z_m^{2^m-1}$ are labelled by $\tilde{\sigma}^{m-1}(a)$.

The Cayley graph of $\mathcal{L}_{\mathbb{F}_2}(\widetilde{\mathfrak{G}})$ is as follows:



with the same labellings as for $L(\widetilde{\mathfrak{G}})$; and power maps from x_m^r to z_m^r.

8. Other Fractal Groups

The technique involved in the proof of the results of the last three sections show that for a group G acting on a tree Σ^* by powers of the cyclic permutation $\epsilon = (0, 1, \ldots, p-1)$ at each vertex, G has finite width when the following conditions are satisfied:

1. the corresponding action on a sequence $\{V_n\}_{n=0}^{\infty}$ of G-modules as defined in Subsection 5.1 has the *bounded corank property*, i.e. there is a constant C such that
$$\dim V_n^r/[G, V_n^r] \leq C$$
for all $n \geq 0$ and $0 \leq r \leq p^n - 1$.
2. There is a descending sequence $\{N_m\}_{m=1}^{\infty}$ of normal subgroups of G satisfying the condition that for all m the quotients N_m/N_{m+1} are isomorphic to some direct sum $\bigoplus_{i=1}^{K} V_{m+\delta_i}$ for fixed K and δ_i.

Let us mention that the p-groups G_ω, for arbitrary $p \geq 2$ and $\omega \in \{0, \ldots, p\}^{\mathbb{N}}$ constructed in [Gri84, Gri85] all satisfy Condition 1. Also, the group $\langle a, t\rangle < \mathsf{Aut}(\Sigma_p^*)$, $p \geq 3$, where a acts as ϵ on the root vertex and trivially elsewhere and t is defined recursively by $t = (a, 1, \ldots, 1, t)$, satisfies Condition 1. We believe that this last group also satifies Condition 2, as do all G_ω for periodic sequences ω. Note that $\mathfrak{G}$ is a particular case of G_ω when $p = 2$ and $\omega = 012012\ldots$. Therefore they all 'should' have finite width.

Meanwhile, the Gupta-Sidki groups constructed in [GS83] do not satisfy Condition 1. As was proved recently by the first author, the growth of the Lie algebra $\mathcal{L}_{\mathbb{F}_p}(G)$ coincides with the spherical growth of the Schreier graph of G relatively to $\mathsf{Stab}_G(e)$, where e is an infinite geodesic path in the tree Σ^*. For our groups $\mathfrak{G}$ and $\widetilde{\mathfrak{G}}$ the spherical growth is bounded and this is why these groups have bounded width. For the Gupta-Sidki groups, the spherical growth of the Schreier graph is unbounded (it grows approximately as $\sqrt{n}$), and therefore these groups do not have the finite width property. It also follows from these considerations that their growth is at least $e^{n^{1-1/(1/2+2)}} = e^{n^{3/5}}$.

9. Profinite Groups of Finite Width

Finally we wish to explain how our results in the previous sections lead to counterexamples to Conjecture 1.1 stated in the introduction. Let $\widehat{G}$ be the profinite completion of $G = \mathfrak{G}$ or $\widetilde{\mathfrak{G}}$.

Theorem 9.1. *The group $\widehat{G}$ is a just-infinite pro-2-group of finite width which does not belong to the list of Conjecture 1.1 (which consists of solvable groups, p-adic analytic groups, and groups commensurable to positive parts of loop groups or to the Nottingham group).*

Its proof relies on the following notion:

Definition 9.2. Let $G < \mathsf{Aut}(\Sigma^*)$ be a group acting on a rooted tree. G has the *congruence subgroup property* if for any finite-index subgroup H of G there is an n such that $\mathsf{Stab}_G(n) < H < G$.

Proof. G has the congruence property. This is well known for $\mathfrak{G}$ (see for instance [Gri00]); while for $\widetilde{\mathfrak{G}}$ the subgroup $\tilde{K}$ contains $\mathsf{Stab}_{\widetilde{\mathfrak{G}}}(4)$ and enjoys the property that every subgroup of finite index in $\widetilde{\mathfrak{G}}$ contains $\tilde{K}_m = \tilde{K} \times \cdots \times \tilde{K}$ for some m; see [BG99].

The profinite completion of G with respect to its subgroups $\mathsf{Stab}_G(n)$ is therefore a pro-2-group and coincides with the closure of G in $\mathsf{Aut}(\{0,1\}^*)$. The closure of a branch group is again a branch group, as is observed in [Gri00].

The criterion of just-infiniteness for profinite branch groups is the same as the one for discrete branch groups given in [BG99]; it is that $\overline{K}/\overline{K}'$ (respectively $\overline{\tilde{K}}/\overline{\tilde{K}}'$) be finite, where $\overline{K}$ and $\overline{\tilde{K}}$ are the closures of K and $\tilde{K}$. Now $|\overline{K}/\overline{K}'| \leq |K/K'| < \infty$, the last inequality following from a computation in [BG99]. The same inequalities hold for $\widetilde{\mathfrak{G}}$, and this proves the just-infiniteness of $\widehat{G}$.

The group $\widehat{G}$ has finite width for both versions of Definition 1.2. This is clear for D-width, because the discrete and pro-p Lie algebras $\mathcal{L}(G)$ and $\mathcal{L}(\widehat{G})$ are isomorphic. The finiteness of C-width follows from the inequalities

$$\left|\gamma_n(\widehat{G})/\gamma_{n+1}(\widehat{G})\right| \leq |\gamma_n(G)/\gamma_{n+1}(G)| < \infty,$$

which again are consequences of the congruence property of G.

Finally, $\widehat{G}$ does not belong to the list of groups given in Conjecture 1.1: it is neither solvable, because G isn't, nor p-adic analytic, by Lazard's criterion [Laz65] (its Lie algebra $\mathcal{L}(\widehat{G}) = \mathcal{L}(G)$ would have a zero component in some dimension). The other groups in the list of Conjecture 1.1 are *hereditarily just-infinite* groups, that is, groups every open subgroup of which is just-infinite [KLP97, page 5]. Profinite just-infinite branch groups are never hereditarily just-infinite, as is shown in [Gri00]. ☐

Laurent Bartholdi Rostislav Grigorchuk

Section de Mathématiques
Université de Genève
CP 240, 1211 Genève 24
Switzerland
`Laurent.Bartholdi@math.unige.ch`

Steklov Mathematical Institute
Gubkina Street 8
Moscow 117966
Russia
`grigorch@mi.ras.ru`

References

[And76] George E. Andrews, *The theory of partitions*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976, Encyclopedia of Mathematics and its Applications, Vol. 2.

[Bar98] Laurent Bartholdi, *The growth of Grigorchuk's torsion group*, Internat. Math. Res. Notices **20** (1998), 1049–1054.

[Bas72] Hyman Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. London Math. Soc. (3) **25** (1972), 603–614.

[Ber83] Alexander E. Berezniĭ, *Discrete subexponential groups*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **123** (1983), 155–166 (Russian).

[BG99] Laurent Bartholdi and Rostislav I. Grigorchuk, *On parabolic subgroups and Hecke algebras of some fractal groups*, submitted to Proc. Conf. Bielefeld, 1999, math.GR/9911206.

[Bok63] Leonid A. Bokut', *A basis for free polynilpotent Lie algebras*, Algebra i Logika Sem. **2** (1963), no. 4, 13–19.

[CG97] Tullio G. Ceccherini-Silberstein and Rostislav I. Grigorchuk, *Amenability and growth of one-relator groups*, Enseign. Math. (2) **43** (1997), no. 3-4, 337–354.

[DdSMS91] John D. Dixon, Marcus P. F. du Sautoy, Avinoam Mann, and Dan Segal, *Analytic pro-p-groups*, Cambridge University Press, Cambridge, 1991.

[Ego84] Georgiĭ P. Egorychev, *Integral representation and the computation of combinatorial sums*, American Mathematical Society, Providence, R.I., 1984, Translated from the Russian by H. H. McFadden, Translation edited by Lev J. Leifman.

[GH97] Rostislav I. Grigorchuk and Pierre de la Harpe, *On problems related to growth, entropy, and spectrum in group theory*, J. Dynam. Control Systems **3** (1997), no. 1, 51–89.

[Gol64] Evgueniĭ S. Golod, *On nil-algebras and finitely approximable p-groups*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 273–276.

[Gri80] Rostislav I. Grigorchuk, *On Burnside's problem on periodic groups*, Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 53–54, English translation: Functional Anal. Appl. **14** (1980), 41–43.

[Gri84] Rostislav I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no. 5, 939–985, English translation: Math. USSR-Izv. **25** (1985), no. 2, 259–300.

[Gri85] Rostislav I. Grigorchuk, *Degrees of growth of p-groups and torsion-free groups*, Mat. Sb. (N.S.) **126(168)** (1985), no. 2, 194–214, 286.

[Gri89] Rostislav I. Grigorchuk, *On the Hilbert-Poincaré series of graded algebras that are associated with groups*, Mat. Sb. **180** (1989), no. 2, 207–225, 304, English translation: Math. USSR-Sb. **66** (1990), no. 1, 211–229.

[Gri00] Rostislav I. Grigorchuk, *Just infinite branched groups*, Horizons in Profinite Groups (Dan Segal, Markus P. F. du Sautoy, and Aner Shalev, eds.), Birkhaüser, Basel, 2000, pp. 121–179.

[Gro81a] Mikhael Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 53, 53–73.

[Gro81b] Mikhael Gromov, *Structures métriques pour les variétés riemanniennes*, CEDIC, Paris, 1981, Edited by J. Lafontaine and P. Pansu.

[GS64] Evgueniĭ S. Golod and Igor R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), no. 2, 261–272 (Russian).

[GS83] Narain D. Gupta and Said N. Sidki, *On the Burnside problem for periodic groups*, Math. Z. **182** (1983), 385–388.

[Gui70] Yves Guivarc'h, *Groupes de Lie à croissance polynomiale*, C. R. Acad. Sci. Paris Sér. A-B **271** (1970), A237–A239.

[Gui73] Yves Guivarc'h, *Croissance polynomiale et périodes des fonctions harmoniques*, Bull. Soc. Math. France **101** (1973), 333–379.

[Har00] Pierre de la Harpe, *Topics in geometric group theory*, University of Chicago Press, 2000.

[HB82] Bertram Huppert and Norman Blackburn, *Finite groups II*, Springer-Verlag, Berlin, 1982, AMD, 44.

[Her94] Israel N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs, vol. 15, Mathematical Association of America, Washington, DC, 1994, Reprint of the 1968 original, With an afterword by Lance W. Small.

[Jac41] Nathan Jacobson, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **50** (1941), 15–25.

[Jac62] Nathan Jacobson, *Lie algebras*, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962, Interscience Tracts in Pure and Applied Mathematics, No. 10.

[Jen41] Stephen A. Jennings, *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.

[Jen55] Stephen A. Jennings, *The group ring of a class of infinite nilpotent groups*, Canad. J. Math. **7** (1955), 169–187.

[Kaĭ80] Vadim A. Kaĭmanovič, *The spectral measure of transition operator and harmonic functions connected with random walks on discrete groups*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **97** (1980), 102–109, 228–229, 236, Problems of the theory of probability distributions, VI.

[Kal46] Lev A. Kaloujnine, *Sur les p-groupes de Sylow du groupe symétrique du degré p^m. (Suite centrale ascendante et descendante.)*, C. R. Acad. Sci. Paris Sér. I Math. **223** (1946), 703–705.

[Kes59] Harry Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959), 336–354.

[KLP97] Gundel Klaas, Charles R. Leedham-Green, and Wilhelm Plesken, *Linear pro-p-groups of finite width*, Lecture Notes in Mathematics, vol. 1674, Springer-Verlag, Berlin, 1997.

[Koc70] Helmut Koch, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag, Berlin, 1970, Mit einem Geleitwort von I. R. Šafarevič.

[Kou98] Malik Koubi, *Croissance uniforme dans les groupes hyperboliques*, to appear, 1998.

[Laz53] Michel Lazard, *Sur les groupes nilpotents et les anneaux de lie*, Ann. École Norm. Sup. (3) **71** (1953), 101–190.

[Laz65] Michel Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.

[Leo98] Yuriĭ G. Leonov, *On lower estimation of growth for some torsion groups*, to appear, 1998.

[LG94] Charles R. Leedham-Green, *The structure of finite p-groups*, J. London Math. Soc. (2) **50** (1994), no. 1, 49–67.

[LM91] Alexander Lubotzky and Avinoam Mann, *On groups of polynomial subgroup growth*, Invent. Math. **104** (1991), no. 3, 521–533.

[Mag40] Wilhelm Magnus, *Über Gruppen und zugeordnete Liesche Ringe*, J. Reine Angew. Math. **182** (1940), 142–149.

[Mei54] Günter Meinardus, *Asymptotische Aussagen über Partitionen*, Math. Z. **59** (1954), 388–398.

[Mil68] John W. Milnor, *Growth of finitely generated solvable groups*, J. Differential Geom. **2** (1968), 447–449.

[MZ99] Consuelo Martinez and Efim I. Zel'manov, *Nil algebras and unipotent groups of finite width*, To appear in Advances in Math., 1999.

[Pas77] Donald S. Passman, *The algebraic structure of group rings*, Wiley-Interscience [John Wiley & Sons], New York, 1977, Pure and Applied Mathematics.

[Pas79] Inder Bir S. Passi, *Group rings and their augmentation ideals*, Lecture Notes in Mathematics, vol. 715, Springer, Berlin, 1979.

[Pet93] Victor M. Petrogradskiĭ, *Some type of intermediate growth in Lie algebras*, Uspekhi Mat. Nauk **48** (1993), no. 5(293), 181–182.

[Pet96] Victor M. Petrogradskiĭ, *Intermediate growth in Lie algebras and their enveloping algebras*, J. Algebra **179** (1996), no. 2, 459–482.

[Qui68] Daniel G. Quillen, *On the associated graded ring of a group ring*, J. Algebra **10** (1968), 411–418.

[Roz96a] Alexander V. Rozhkov, *Lower central series of a group of tree automorphisms*, Mat. Zametki **60** (1996), no. 2, 225–237, 319.

[Roz96b] Alexander V. Rozhkov, *Conditions of finiteness in groups of automorphisms of trees*, Habilitation thesis, Chelyabinsk, 1996.

[Sha95a] Aner Shalev, *Finite p-groups*, Finite and locally finite groups (Istanbul, 1994), Kluwer Acad. Publ., Dordrecht, 1995, pp. 401–450.

[Sha95b] Aner Shalev, *Some problems and results in the theory of pro-p groups*, Groups '93 Galway/St. Andrews, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, pp. 528–542.

[Tit72] Jacques Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

[VZ93] Michael Vaughan-Lee and Efim I. Zel'manov, *Upper bounds in the restricted Burnside problem*, J. Algebra **162** (1993), no. 1, 107–145.

[VZ96] Michael Vaughan-Lee and Efim I. Zel'manov, *Upper bounds in the restricted Burnside problem. II*, Internat. J. Algebra Comput. **6** (1996), no. 6, 735–744.

[Wol68] Joseph A. Wolf, *Growth of finitely generated solvable groups and curvature of Riemanniann manifolds*, J. Differential Geom. **2** (1968), 421–446.

[Zas40] Hans Zassenhaus, *Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Characteristik p zuzuordnen*, Abh. Math. Sem. Univ. Hamburg **13** (1940), 200–207.

[Zel95a] Efim I. Zel'manov, *Lie ring methods in the theory of nilpotent groups*, Groups '93 Galway/St. Andrews, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, pp. 567–585.

[Zel95b] Efim I. Zel'manov, *More on Burnside's problem*, Combinatorial and geometric group theory (Edinburgh, 1993), London Math. Soc. Lecture Note Ser., vol. 204, Cambridge Univ. Press, Cambridge, 1995, pp. 314–321.

[Zel96] Efim I. Zel'manov, *Talk at the ESF conference on algebra and discrete mathematics "Group Theory: from Finite to Infinite"*, Castelvecchio Pascoli, 13–18 July 1996.

[Zel97] Efim I. Zel'manov, *On the restricted Burnside problem*, Fields Medallists' lectures, World Sci. Ser. 20th Century Math., vol. 5, World Sci. Publishing, River Edge, NJ, 1997, pp. 623–632.